



REPLY TO  
ATTENTION OF

**DEPARTMENT OF THE ARMY**  
HEADQUARTERS, U.S. ARMY MATERIEL COMMAND  
9301 CHAPEK ROAD  
FORT BELVOIR, VA 22060-5527

AMCIO-P

05-07-AMCIO-P  
22 May 2005

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Policy Letter - Appointment of Designated Approval Authority (DAA)

1. References:

a. DoDI 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP).

b. AR 25-2, 14 November 2003, Information Assurance.

2. The U.S. Army Materiel Command (AMC) Chief Information Officer (CIO)/G-6 and the Major Subordinate Command (MSC) Commanders are the Designated Approval Authority (DAA) for certification and accreditation of information applications and networks within their operational area of responsibility. This authority will be exercised within the limits established by the references and as further specified below:

a. The AMC CIO/G-6 may, at his discretion, certify and accredit (or rescind such approval) for any application or network within AMC's area of responsibility as authorized by the references.

b. AMC CIO/G6 will be sole DAA for all Top Secret (TS) collateral and Special Access Programs (SAPS) systems within AMC. The sponsoring agency will serve as the Certification Technical Authority.

c. MSC commanders may certify and accredit only those applications and networks within their area of responsibility operating, at the Secret and below and Sensitive (Unclassified) levels.

d. Addressees may further delegate this DAA, in writing, as follows:

(1) Secret and below: The DAA will be at minimum a colonel (O-6) or GS-15 who is occupying a position of Command or a principal staff office at an installation or general officer Command.

(2) Sensitive (Unclassified): The DAA will be at the minimum a lieutenant colonel or GS-14.

AMCIO-P

SUBJECT: Policy Letter – Appointment of Designated Approval Authority (DAA)

3. All systems that process sensitive or classified information require certification and accreditation. There are two aspects of approval covered by this delegation: type accreditation (for individual applications) and network accreditation. Type accreditation applies to applications developed for other than a single implementation, i.e., for multiple instances across multiple networks. Applications intended for wide release are accredited by the developing agency independent of a specific network (type accreditation). Using agencies rely on a type accreditation when performing their network accreditation. AMC network accreditation applies to networks controlled by AMC and should be done in concert with the garrison Director of Information Management as applicable.
4. DAA's will provide a copy of the letter of appointment (to include the level of system classification) to Headquarters, AMC, ATTN: AMCIO-P. The AMC CIO/G-6 will ensure that DAA's meet training requirements and operate within the scope of their authority. AMC CIO/G-6 will provide oversight for the Command Defense Information Technology Security Certification and Accreditation Process (DITSCAP).
5. This designated authority is granted to the positions specified above and not solely to the current incumbent. This delegation rescinds all previous DAA designations and will remain in effect until modified or rescinded by Commander, U.S. Army Materiel Command.
6. Any questions or concerns should be referred to G-6, Information Assurance Program Manager (AMCIO-P), [amcio-iapm@hqamc.army.mil](mailto:amcio-iapm@hqamc.army.mil) at 703-806-8824 or DSN 656-8824.

//Signed//  
BENJAMIN S. GRIFFIN  
General, USA  
Commanding

DISTRIBUTION:

B  
H